REMARKS

Claims 1-17 are pending in the present application, of which claims 1, 8, 11, 15 and 17 are independent. No amendments have been made. Applicants believe that the present application is in condition for allowance, and respectfully request the Examiner to reconsider the rejection in light of the remarks set forth below.

I. REJECTION UNDER 35 U.S.C. §102

The Examiner maintained rejection of claims 1, 2 and 5 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 6,609,199 issued to DeTreville (hereinafter "DeTreville"). The rejection is respectfully traversed in its entirety.

> To anticipate a claim under 35 U.S.C. §102(e), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (see MPEP §2131).

In the Office Action, the Examiner states that DeTreville teaches generating a plurality of keys in response to a received challenge from the portable IC device and, more particularly, cites column 5, lines 54-65. Upon review of the cited portion, Applicants disagree.

DeTreville teaches CPU manufacturer to equip the CPU with a pair of public and private key (col. 5, lines 54-55). Accordingly, the keys are stored onto the CPU at the time of manufacturing. The already stored private key is then use when responding to the challenges from a portable IC device. This means that the keys are not generated in response to a received challenge. The keys are used in response to a received challenge. Therefore, DeTreville does not teach or even suggest generating a plurality of keys in response to a received challenge.

Since DeTreville does not teach at least the above element of claim 1, Applicants submit that DeTreville does not teach all elements of claim 1 and therefore, claim 1 is allowable. Also,

claims 2 and 5 depend from and include all the elements cited in the independent claim 1. Accordingly, Applicant submits that these claims are believed to be allowable based on their dependency from an allowable base claim as well as other novel features included therein.

For at least the foregoing reasons, Applicants respectfully request a withdrawal of the rejection under 35 U.S.C. §102.

II. REJECTION UNDER 35 U.S.C. §102

The Examiner rejected claims 8-13, 15 and 17 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 6,516,414 issued to Zhang et al. (hereinafter "Zhang"). Again, the rejection is respectfully traversed in its entirety.

Zhang teaches an improved authorization process for a conditional access system (See Background). It discusses various cryptographic concepts (see col. 2, lines 17-40) and teaches a content protection system using concatenation of various parameters (see col. 7, line 7 to col. 8, line 1 and col. 8, lines 33-37). Particularly, in the portion cited by the Examiner, Zhang discloses concatenation performed with respect to a random number M_H or M_P, a device identifier P_ID or H_ID and a binding message $G^{-(P+H)} \bmod N$ (see col. 8, lines 32-62). Upon review, there is nothing in Zhang to suggest a concatenation of a secret key with information from a mobile unit as in claim 8.

Moreover, Zhang teaches various embodiments for derivation of a session key K that can be used for ciphering broadcast programming. It teaches a third entity that is involved to perform entity authentication and session key derivation (see col. 3, line 64 to col. 4, line 17). In one embodiment, a shared key k and shared session key K are derived based on ElGamal algorithm (see col. 9, line 27 to col. 10, line 5). In another embodiment, a one-way hash function

algorithm is used in the derivation of the keys k and K (col. 11, lines 10-14). However, there is nothing in Zhang to suggest a generation of a signature as in claim 8

With respect to claim 11, Zhang teaches derivation of shared key k and a shared session key K using the shared key k such that content for transmission can be ciphered using the shared session key K (see col. 12, lines 17-20, lines 34-39 and lines 45-54). Namely, both keys k and K are derived. This means that a communication key is not delivered. Therefore, Zhang does not teach delivering a communication key to a communications unit as in claim 11. In the portion cited by the Examiner, Zhang teaches computing a hash function with respect to a common initial counter value N and a secret key P or H (see col. 11, lines 50-53 and lines 55-56). Zhang does not teach or even suggest hashing with respect to an authorization message as in claim 11.

With respect to claim 15, Zhang does not teach transmitting a key to a communications device and generating a signature as discussed above. In addition, upon review of the portions cited by the Examiner, Applicants submit that Zhang does not even mention a signature generation. Therefore, it does not teach transmitting a signature, receiving a signature and generating a primary signature from a received signature as in claim 11.

Finally, Zhang does not teach or even suggest generating a primary signature based on a key that is held private from a mobile station and a secondary signature that is received from the mobile station as in claim 17. The portion cited by the Examiner discusses generation of the session keys. It does not discuss an apparatus communicatively coupled to a mobile station, wherein the apparatus comprises a memory and a processor. Moreover, there is no mention of generating a signature.

Since Zhang does not teach at least the above elements of the respective claims, Applicants submit that Zhang does not teach all elements of the claims and therefore, claims 8, 11, 15 and 17 are allowable. Also, claims 9-10 and 12-13 depend from and include all the

elements cited in the independent claims 8 and 11 respectively. Accordingly, Applicant submits that these claims are believed to be allowable based on their dependency from an allowable base claim as well as other novel features included therein.

For at least the foregoing reasons, Applicants respectfully submit that Zhang does not teach every element of the claims and request a withdrawal of the rejection under 35 U.S.C. §102.

III. REJECTION UNDER 35 U.S.C. §103

The Examiner rejected claims 3, 4, 6 and 7 under 35 U.S.C. §103 as being unpatentable over DeTreville in view of U.S. Patent No. 6,076,162 issued to Deindl et al. (hereinafter "Deindl"). The Examiner also rejected claims 14 and 16 under 35 U.S.C. §103 as being unpatentable over Zhang in view of Applied Cryptography (hereinafter Schneier).

> To establish a prima facie case of obviousness for a claimed invention, all the claim elements must be taught or suggested by the prior art. (MPEP 2143.03)

Claims 3, 4, 6 and 7 depend from and include all the elements cited in the independent claim 1. Accordingly, Applicants submit that DeTreville does not disclose every element of claims 3, 4, 6 and 7 based on its dependency from claim 1 as well as other novel features included therein. Although not relied upon, Deindl also does not teach the concatenation as in independent claim 1.

Since neither DeTreville nor Deindl, separately or combined, teach or suggest all the elements, Applicants respectfully submit that the Examiner has failed to set forth a prima facie case of obviousness and respectfully request that the rejections of claims 3, 4, 6 and 7 be withdrawn.

Similarly, claims 14 and 16 depend from and include all the elements cited in the independent claims 11 and 15, respectively. Accordingly, Applicants submit that Zhang does not disclose every element of claims 14 and 16 based on its dependency from claims 11 and 15 as well as other novel features included therein. Therefore, Applicants respectfully submit that the Examiner has failed to set forth a prima facie case of obviousness and respectfully request that the rejections of claims 14 and 16 be withdrawn.

Attorney Docket No. 010055B1

CONCLUSION

In light of the amendments contained herein, Applicants submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: January 23, 2006

By: _____
Jae-Hee Choi, Reg. No. 45,288
(858) 651-5469

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502